

Rec'd PCT/PTO 03 DEC 2004

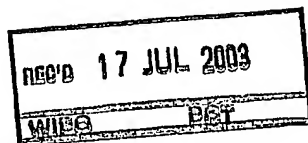
20/516846

PCT/IB 03/02583

04.06.03



INVESTOR IN PEOPLE



The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ

**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

BEST AVAILABLE COPY

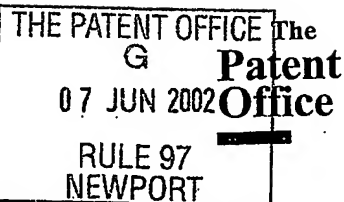
Signed

Dated 14 March 2003



An Executive Agency of the Department of Trade and Industry

Form 1/77

Patents Act 1977  
(Rule 16)

1/77

11JUN02 E724618-3 002879  
P01/7700 0.00-0213242.1**Request for grant of a patent***(See notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)*The Patent Office  
Cardiff Road  
Newport  
Gwent NP10 8QQ

1. Your reference PHNL020535
- 
2. Patent application number 0213242.1 07 JUN 2002  
*(The Patent Office will fill in this part)*
- 
3. Full name, address and postcode of the or of each applicant *(underline all surnames)* KONINKLIJKE PHILIPS ELECTRONICS N.V.  
GROENEWOUDSEWEG 1  
5621 BA EINDHOVEN  
THE NETHERLANDS
- Patents ADP Number *(if you know it)* 7419294001
- If the applicant is a corporate body, give the country/state of its incorporation THE NETHERLANDS
- 
4. Title of the invention AES MIXCOLUMN TRANSFORM
- 
5. Name of your agent *(if you have one)* Brian T. STEVENS  
"Address for service" in the United Kingdom Philips Intellectual Property and Standards  
to which all correspondence should be sent Cross Oak Lane  
*(including the postcode)* Redhill  
Surrey RH1 5HA
- Patents ADP number *(if you know it)* 8359655001
- 
- |   |         |  |   |
|---|---------|--|---|
| 6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and <i>(if you know it)</i> the or each application number | Country | Priority Application number<br><i>(if you know it)</i> | Date of filing<br><i>(day/month/year)</i> |
|---|---------|--|---|
- 
- |   |                               |   |
|---|-------------------------------|---|
| 7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application | Number of earlier application | Date of filing<br><i>(day/month/year)</i> |
|---|-------------------------------|---|
- 
8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer "Yes" if:*  
a) *any applicant named in part 3 is not an inventor, or*  
b) *there is an inventor who is not named as an applicant, or*  
c) *any named applicant is a corporate body.*  
See note (d))
- YES

Patents form 1/77

**Patents Form 1/77**

9. Enter the number of sheets for any of the following items you are filing with this form.  
Do not count copies of the same document.

Continuation sheets of this form

Description	10
Claims(s)	3
Abstract	1
Drawings	2

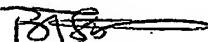
10. If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents  
Statement of inventorship and right  
to grant of a patent (*Patents Form 7/77*)  
Request for preliminary examination and  
search (*Patents Form 9/77*)  
Request for substantive examination  
(*Patents Form 10/77*)  
Any other documents  
(*Please specify*)

11. I/We request the grant of a patent on the basis of this application.

Signature



Date 06-06-2002

12. Name and daytime telephone number of person to contact in the United Kingdom
- |              |             |
|--------------|-------------|
| 01293 815492 | (R. Turner) |
|--------------|-------------|

**Warning**

*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.*

**Notes**

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered "Yes" *Patents Form 7/77* will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

## DESCRIPTION

## AES MIXCOLUMN TRANSFORM

5

The present invention relates to methods and apparatus for implementation of the Advanced Encryption Standard (AES) algorithm and in particular to methods and apparatus for performing the matrix multiplication operation that constitutes the AES MixColumn transformation in each of the encryption and decryption rounds of the algorithm.

The invention has particular, though not exclusive, application in cryptographic devices such as those installed in smart cards and other devices where processor and memory resources are somewhat limited and many operations of the cryptographic algorithm are performed in dedicated ASIC or FPGA hardware.

The AES algorithm has wide application in the encryption of data to be transmitted in a secure fashion. One application is in the transmittal of personal and/or financial information from a smartcard to a card reader device. Confidential data stored on the card must not be retrieved from the card except in encrypted form to ensure that the data so retrieved cannot be intercepted and read by an unauthorised third party. Only the authorised reader is able to decrypt the data retrieved from the card.

Similarly, data supplied by the card reader to be stored in the card must be passed to the card in encrypted form, and decrypted by the card for storage and subsequent retrieval.

While the AES algorithm is relatively straightforward to implement in a conventional computer system deploying state of the art processor and memory circuits, in a smartcard application, the processor and memory resource is very limited, and many functions must be executed in dedicated hardware, such as ASICs or FPGAs.

There is therefore a requirement for hardware implementations of the procedures required in the AES algorithm which implementations require the minimum use of hardware resource.

5 It is an object of the present invention to provide suitable circuitry for effecting the MixColumn transform deployed in the standard AES (Rijndael) cryptographic algorithm, both for encryption and decryption.

According to one aspect, the present invention provides a logic circuit for multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  
10  $m$  is a number of rows and  $n$  is a number of columns, and wherein each successive row  $m$ , of  $n$  elements is a predetermined row permutation of a preceding row, the circuit comprising:

$n$  multiplication circuits each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

15  $n$  logic circuits, each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the  $n$  multiplication circuits;

$n$  registers for receiving said logical output;

20 feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.

25 Embodiments of the present invention will now be described by way of example and with reference to the accompanying drawings in which:

Figure 1 is a flow diagram illustrating implementation of an encryption operation using the AES block cipher algorithm; and

30 Figure 2 is a schematic diagram of a functional logic block for performing the MixColumns transform.

The AES algorithm for encryption of plaintext to ciphertext is shown in figure 1. The AES algorithm may be implemented using a 128-bit, a 192-bit or a 256-bit key operating on successive 128-bit blocks of input data. The present invention is applicable to all of these implementations. Figure 1 will  
5 now be described in the context of the basic implementation using a 128-bit key.

An initial 128-bit block of input plaintext 10 is XOR-combined 11 with an original 128-bit key 12 in an initial round 15. The output 13 from this initial round 15 is then passed through a number of repeated transform stages, in an  
10 encryption round 28 which includes the SubBytes transform 20, the ShiftRows transform 21 and the MixColumns transform 22 in accordance with the defined AES algorithm.

The output from the MixColumns transform 22 is XOR-combined 23 with a new 128-bit round key 26, which has been derived 25 from the initial (original) key 12. The output from this XOR-combination 23 is fed back to pass through the encryption round 28 a further number of times, the number depending upon the particular implementation of the algorithm.

For each successive iteration through the encryption round 28, a new round key 26' is derived from the existing round key 26 according to the AES  
20 round key schedule.

The number of iterations ( $N_r - 1$ ) of the encryption round 28 is nine where a 128-bit encryption key is being used, eleven where a 192-bit encryption key is being used, and thirteen where a 256-bit encryption key is being used.

25 After the requisite number ( $N_r - 1$ ) of encryption rounds 28, a final round,  $N_r$ , is entered under the control of decision box 24. The final round 30 comprises a further SubBytes transform 31, a further ShiftRows transform 32, and a subsequent XOR-combination 33 of the result with a final round key 36 generated 35 from the previous round key. The output therefrom comprises  
30 the ciphertext output 39 of the encryption algorithm.

The present invention relates particularly to the performing of the MixColumns transform 22. Through the rounds 28, 30, the 128-bit blocks

being processed are conveniently represented as 16 8-bit blocks in a  $4 \times 4$  matrix, as  $s_{\text{row}, \text{column}}$ , according to the pattern,

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

5

In the MixColumns transform 22, the columns of this state are considered as polynomials over  $\text{GF}(2^8)$  and multiplied modulo  $(x^4 + 1)$  with a predetermined fixed polynomial  $a(x)$ , given by:

10

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0,$$

in which, represented as hexadecimal values,

15

$$a_3 = 03 \text{ h}$$

$$a_2 = 01 \text{ h}$$

$$a_1 = 01 \text{ h}$$

$$a_0 = 02 \text{ h.}$$

20

The polynomial is co-prime to  $x^4 + 1$  and is therefore invertible.

For encryption, the MixColumns transform can therefore be expressed as

$$s_{r,c} \rightarrow s'_{r,c}, \text{ for each of the columns in } s.$$

25

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix}$$

The evaluation of this matrix multiplication is:

5

$$\begin{aligned} s'_{0,c} &= \{02\} * s_{0,c} \oplus \{03\} * s_{1,c} \oplus s_{2,c} \oplus s_{3,c} \\ s'_{1,c} &= s_{0,c} \oplus \{02\} * s_{1,c} \oplus \{03\} * s_{2,c} \oplus s_{3,c} \\ s'_{2,c} &= s_{0,c} \oplus s_{1,c} \oplus \{02\} * s_{2,c} \oplus \{03\} * s_{3,c} \\ 10 \quad s'_{3,c} &= \{03\} * s_{0,c} \oplus s_{1,c} \oplus s_{2,c} \oplus \{02\} * s_{3,c} \end{aligned}$$

During decryption, the inverse of this operation is required. It is given by the following matrix multiplication.

15

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} b_0 & b_3 & b_2 & b_1 \\ b_1 & b_0 & b_3 & b_2 \\ b_2 & b_1 & b_0 & b_3 \\ b_3 & b_2 & b_1 & b_0 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0B & 09 \\ 09 & 0E & 0E & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix}$$

The evaluation of this matrix multiplication is:

$$\begin{aligned} 20 \quad s'_{0,c} &= \{0E\} * s_{0,c} \oplus \{0B\} * s_{1,c} \oplus \{0D\} * s_{2,c} \oplus \{09\} * s_{3,c} \\ s'_{1,c} &= \{09\} * s_{0,c} \oplus \{0E\} * s_{1,c} \oplus \{0B\} * s_{2,c} \oplus \{0D\} * s_{3,c} \\ s'_{2,c} &= \{0D\} * s_{0,c} \oplus \{09\} * s_{1,c} \oplus \{0E\} * s_{2,c} \oplus \{0B\} * s_{3,c} \\ s'_{3,c} &= \{0B\} * s_{0,c} \oplus \{0D\} * s_{1,c} \oplus \{09\} * s_{2,c} \oplus \{0E\} * s_{3,c} \end{aligned}$$



It is noted that the MixColumns transform matrix has the special property that each successive row is a shifted or rotated version of the preceding row. In general, each element in a row appears in every row but in a different position in the row, and specifically, for the MixColumns transform  
5 matrix the different position of each element for each row constitutes a single position right shift or rotation.

According to the present invention, it has been recognised that this property allows the multiplication of each column of the state  $s$  to be achieved with significantly reduced hardware.

10 Figure 2 illustrates an exemplary embodiment of hardware logic 50 adapted for the multiplication of an  $m \times n$  matrix by a  $1 \times n$  matrix, in which the relationship between each successive row of  $n$  elements of the  $m \times n$  matrix is a predetermined row shift. For the AES MixColumns transform,  $m = 4$ ,  $n = 4$  and the predetermined relationship is a single right shift.

15 The logic 50 comprises four 8-bit multiplication circuits 60 ... 63, four 8-bit XOR gates 70 ... 73 and four feedback / output registers 80 ... 83, shown as MixCol<sub>0</sub> ... MixCol<sub>3</sub>. Each multiplication circuit 70 ... 73 is adapted for multiplication of an input by one of the matrix coefficients  $c_0, c_1, c_2, c_3$ . Each of  
20 the XOR gates 70 ... 73 may be implemented using any appropriate combination of logic elements required to execute the appropriate logical combination of two inputs, as described hereinafter.

For encryption rounds, the values of  $c_0 \dots c_3$  are, respectively,  $a_0 \dots a_3$  as defined above. For decryption rounds, the values of  $c_0 \dots c_3$  are,  
25 respectively,  $b_0 \dots b_3$  as defined above. The output of each multiplication circuit 60 ... 63 is coupled to a first input of a corresponding XOR gate 70 ... 73. The output of each XOR gate 70 ... 73 is coupled to a corresponding MixCol register 80 ... 83. The output of each MixCol register 80 ... 83 is coupled to the second input of one of the XOR gates 70 ... 73 according to a  
30 feedback plan 90 ... 93 that corresponds to the row shift function that defines the relationship between successive rows of the matrix. In the present case, the feedback plan 90 ... 93 implements the right row shift function between

successive rows of the matrices  $a_{r,c}$  (encryption) and  $b_{r,c}$  (decryption) – more generally the matrix  $c_{r,c}$ .

During operation of the circuit 50,  $s_{0c}$ ,  $s_{1c}$ ,  $s_{2c}$ ,  $s_{3c}$  are sequentially offered to the multiplication logic 60 ... 63 on successive cycles. At the outset of each column multiplication, the registers MixCol<sub>0</sub> to MixCol<sub>3</sub> are pre-set to zero.

*After the 1<sup>st</sup> cycle:*

$$\begin{aligned} \text{MixCol}_0 &= c_{0,0} \cdot s_{0c} \\ 10 \quad \text{MixCol}_1 &= c_{1,0} \cdot s_{0c} \\ \text{MixCol}_2 &= c_{2,0} \cdot s_{0c} \\ \text{MixCol}_3 &= c_{3,0} \cdot s_{0c} \end{aligned}$$

*After the 2<sup>nd</sup> cycle:*

$$\begin{aligned} 15 \quad \text{MixCol}_0 &= c_{0,0} \cdot s_{1c} \oplus c_{1,0} \cdot s_{0c} \\ \text{MixCol}_1 &= c_{1,0} \cdot s_{1c} \oplus c_{2,0} \cdot s_{0c} \\ \text{MixCol}_2 &= c_{2,0} \cdot s_{1c} \oplus c_{3,0} \cdot s_{0c} \\ \text{MixCol}_3 &= c_{3,0} \cdot s_{1c} \oplus c_{0,0} \cdot s_{0c} \end{aligned}$$

20 *After the 3<sup>rd</sup> cycle:*

$$\begin{aligned} \text{MixCol}_0 &= c_{0,0} \cdot s_{2c} \oplus c_{1,0} \cdot s_{1c} \oplus c_{2,0} \cdot s_{0c} \\ \text{MixCol}_1 &= c_{1,0} \cdot s_{2c} \oplus c_{2,0} \cdot s_{1c} \oplus c_{3,0} \cdot s_{0c} \\ \text{MixCol}_2 &= c_{2,0} \cdot s_{2c} \oplus c_{3,0} \cdot s_{1c} \oplus c_{0,0} \cdot s_{0c} \\ \text{MixCol}_3 &= c_{3,0} \cdot s_{2c} \oplus c_{0,0} \cdot s_{1c} \oplus c_{1,0} \cdot s_{0c} \end{aligned}$$

25

*After the 4<sup>th</sup> cycle:*

$$\begin{aligned} \text{MixCol}_0 &= c_{0,0} \cdot s_{3c} \oplus c_{1,0} \cdot s_{2c} \oplus c_{2,0} \cdot s_{1c} \oplus c_{3,0} \cdot s_{0c} \\ \text{MixCol}_1 &= c_{1,0} \cdot s_{3c} \oplus c_{2,0} \cdot s_{2c} \oplus c_{3,0} \cdot s_{1c} \oplus c_{0,0} \cdot s_{0c} \\ \text{MixCol}_2 &= c_{2,0} \cdot s_{3c} \oplus c_{3,0} \cdot s_{2c} \oplus c_{0,0} \cdot s_{1c} \oplus c_{1,0} \cdot s_{0c} \\ 30 \quad \text{MixCol}_3 &= c_{3,0} \cdot s_{3c} \oplus c_{0,0} \cdot s_{2c} \oplus c_{1,0} \cdot s_{1c} \oplus c_{2,0} \cdot s_{0c} \end{aligned}$$

Rearranging these outputs, according to the feedback plan 90 ... 93 gives the outputs:

$$\begin{aligned} \text{MixCol}_1 &= s'_{0,c} \\ \text{MixCol}_2 &= s'_{1,c} \\ \text{MixCol}_3 &= s'_{2,c} \\ \text{MixCol}_0 &= s'_{0,c} \end{aligned}$$

which is the required result.

It will be noted that, generally speaking, the number of rows,  $m$ , in the matrix determines the number of cycles required, while the number of columns,  $n$ , determines the number of logic groups (multipliers 60 ... 63, XOR gates 70 ... 73, and registers 80 ... 83) required.

The multiplication logic 60 ... 63 can be implemented using any suitable logic. In a preferred embodiment, the logic is provided for both encryption and decryption combining certain logic according to the following schedule.

For  $c_0 \times s_{0,c}$ , the output from the respective multiplication logic 60 ... 63 is defined as  $e_{\text{cycle, bit}}$ , and  $d = 0$  for encryption and  $d = 1$  for decryption:

$$\begin{aligned} e_{07} &= s_6 \text{ XNOR NAND}(d, s_{45}) \\ e_{06} &= s_5 \text{ XNOR NAND}(d, s_{347}) \\ e_{05} &= s_4 \text{ XNOR NAND}(d, s_{236}) \\ e_{04} &= s_{37} \text{ XNOR NAND}(d, s_{125}) \\ e_{03} &= s_{27} \text{ XNOR NAND}(d, s_{0157}) \\ e_{02} &= s_{17} \text{ XNOR NAND}(d, s_{0567}) \\ e_{01} &= s_0 \text{ XNOR NAND}(d, s_{87}) \\ e_{01} &= s_7 \text{ XNOR NAND}(d, s_{56}) \end{aligned}$$

Similarly, for  $c_1 \times s_{1,c}$ :

$$e_{17} = s_7 \text{ XNOR NAND}(d, s_4)$$

$$\begin{aligned}
 e_{16} &= s_6 \text{ XNOR NAND}(d, s_{37}) \\
 e_{15} &= s_5 \text{ XNOR NAND}(d, s_{267}) \\
 e_{14} &= s_4 \text{ XNOR NAND}(d, s_{1567}) \\
 e_{13} &= s_3 \text{ XNOR NAND}(d, s_{056}) \\
 5 \quad e_{12} &= s_2 \text{ XNOR NAND}(d, s_{57}) \\
 e_{11} &= s_1 \text{ XNOR NAND}(d, s_6) \\
 e_{10} &= s_0 \text{ XNOR NAND}(d, s_5)
 \end{aligned}$$

Similarly, for  $c_2 \times s_2, c:$

$$\begin{aligned}
 10 \quad e_{27} &= s_7 \text{ XNOR NAND}(d, s_{45}) \\
 e_{26} &= s_6 \text{ XNOR NAND}(d, s_{347}) \\
 e_{25} &= s_5 \text{ XNOR NAND}(d, s_{236}) \\
 e_{24} &= s_4 \text{ XNOR NAND}(d, s_{125}) \\
 15 \quad e_{23} &= s_3 \text{ XNOR NAND}(d, s_{015}) \\
 e_{22} &= s_2 \text{ XNOR NAND}(d, s_{0567}) \\
 e_{21} &= s_1 \text{ XNOR NAND}(d, s_{67}) \\
 e_{20} &= s_0 \text{ XNOR NAND}(d, s_{56})
 \end{aligned}$$

20 Similarly, for  $c_3 \times s_3, c:$

$$\begin{aligned}
 e_{37} &= s_{67} \text{ XNOR NAND}(d, s_4) \\
 e_{36} &= s_{56} \text{ XNOR NAND}(d, s_{37}) \\
 e_{35} &= s_{45} \text{ XNOR NAND}(d, s_{267}) \\
 25 \quad e_{34} &= s_{347} \text{ XNOR NAND}(d, s_{1567}) \\
 e_{33} &= s_{23} \text{ XOR } s_7 \text{ XNOR NAND}(d, s_{056}) \\
 e_{32} &= s_{12} \text{ XOR } s_7 \text{ XNOR NAND}(d, s_{57}) \\
 e_{31} &= s_{01} \text{ XNOR NAND}(d, s_6) \\
 e_{30} &= s_{07} \text{ XNOR NAND}(d, s_5)
 \end{aligned}$$

30

where:

$a_{57} = a_5 \text{ XOR } a_7$   
 $a_{07} = a_0 \text{ XOR } a_7$   
 $a_{34} = a_3 \text{ XOR } a_4$   
 $a_{567} = a_7 \text{ XOR } a_{56}$   
5  $a_{125} = a_{12} \text{ XOR } a_5$   
 $a_{1567} = a_{17} \text{ XOR } a_{56}$   
 $a_{37} = a_3 \text{ XOR } a_7$   
 $a_{67} = a_6 \text{ XOR } a_7$   
 $a_{23} = a_2 \text{ XOR } a_3$   
10  $a_{056} = a_0 \text{ XOR } a_{56}$   
 $a_{267} = a_2 \text{ XOR } a_{67}$   
 $a_{27} = a_2 \text{ XOR } a_7$   
 $a_{56} = a_5 \text{ XOR } a_6$   
 $a_{12} = a_1 \text{ XOR } a_2$   
15  $a_{347} = a_{34} \text{ XOR } a_7$   
 $a_{0157} = a_{01} \text{ XOR } a_{57}$   
 $a_{17} = a_1 \text{ XOR } a_7$   
 $a_{45} = a_4 \text{ XOR } a_5$   
 $a_{01} = a_0 \text{ XOR } a_1$   
20  $a_{236} = a_{23} \text{ XOR } a_6$   
 $a_{0567} = a_{07} \text{ XOR } a_{56}$

This requires 23 XOR gates, 32 XNOR gates and 32 NAND gates.

Other embodiments are intentionally within the scope of the  
25 accompanying claims.

## CLAIMS

1. A logic circuit for multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  $m$  is a number of rows and  $n$  is a number of columns, and wherein each successive row  $m$  of  $n$  elements is a predetermined row permutation of a preceding row, the circuit comprising:
- 5         $n$  multiplication circuits each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;
- 10         $n$  logic circuits, each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the  $n$  multiplication circuits;
- 15         $n$  registers for receiving said logical output;
- feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and
- control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.
- 20        2. The logic circuit of claim 1 in which the feedback logic provides a feedback plan corresponding to said predetermined row permutation that is a row shift.
- 25        3. The logic circuit of claim 2 in which the row shift is a single element right shift.
4. The logic circuit of claim 1 in which the  $n$  logic circuits are each adapted to execute an XOR-combination of said first input and said second input.

5. The logic circuit of claim 1 in which each of the predetermined multiplicands corresponds to one of the elements in the AES Rijndael MixColumns transform function.

5 6. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 02, the multiplicand for the second multiplication circuit = 03, the multiplicand for the third multiplication circuit = 01, and the multiplicand for the fourth multiplication circuit = 01.

10 7. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 0E, the multiplicand for the second multiplication circuit = 0B, the multiplicand for the third multiplication circuit = 0D, and the multiplicand for the fourth multiplication circuit = 09.

15 8. The logic circuit of claim 6 or claim 7 in which the four multiplicands are switchable between the values in claim 6 and the values in claim 7.

20 9. The logic circuit of claim 1 in which the control means is adapted to successively provide as input to each of the  $n$  multiplication circuits each successive element in the  $(1 \times n)$  or  $(m \times 1)$  matrix over each of  $n$  or  $m$  cycles of operation respectively.

25 10. The logic circuit of claim 1 in which each of the  $n$  multiplication circuits, each of the  $n$  logic circuits, and each of the  $n$  registers are at least eight bits wide.

30 11. The logic circuit of claim 1 in which the control means further includes means for providing as output from said logic circuit the contents of the  $n$  registers after each  $n$ th cycle.

12. The logic circuit of claim 1 in which the control means further includes means for resetting each of the registers prior to the first calculation cycle.

5

13. The logic circuit of claim 1 in which each successive row  $m$  of  $n$  elements is a predetermined row permutation of the immediately preceding row.

10

14. An AES MixColumns transform circuit incorporating the logic circuit of any one of claims 1 to 13.

15

15. An AES encryption and/or decryption engine incorporating the logic circuit of any one of claims 1 to 13 for performing the MixColumns transform.

16. Apparatus substantially as described herein with reference to the accompanying drawings.



## ABSTRACT

## AES MIXCOLUMN TRANSFORM

5 A simplified logic circuit for performing the AES Rijndael MixColumns transform exploits the common relationship between each of the successive rows of the transform matrix and its preceding row. A logic circuit for performing multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  $m$  is a number of rows and  $n$  is a number of columns, and where  
10 each successive row,  $m$ , of  $n$  elements is a predetermined row permutation of a preceding row comprises:  $n$  multiplication circuits;  $n$  logic circuits;  $n$  registers for receiving logical output from the logic circuits; feedback logic for routing the contents of each register to a selected one of inputs of the logic circuits in accordance with a feedback plan that corresponds to the common relationship  
15 between successive matrix rows; and control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.

(Figure 2)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**